Vejledning til desktopadministration

Business Desktops

Dokumentets bestillingsnr.: 312947-082

September 2003

Denne vejledning indeholder beskrivelser af og vejledning i brug af funktionen Intelligent Manageability, som er præinstalleret på visse modeller.

ADVARSEL! Tekst, der er fremhævet på denne måde, viser, at hvis du ikke følger vejledningen, kan det medføre personskade eller død.

FORSIGTIG: Tekst, der er fremhævet på denne måde, betyder, at undladelse af at følge de pågældende anvisninger kan medføre beskadigelse af udstyret eller tab af data.

Vejledning til desktopadministration
Business Desktops

Anden udgave (September 2003)
Dokumentets bestillingsnr.: 312947-082

Indholdsfortegnelse

Vejledning til desktopadministration

Indeks

Vejledning til desktopadministration

HP Intelligent Manageability tilbyder standardløsninger til håndtering og kontrol af skriveborde, arbejdsstationer og bærbare computere i et netværksmiljø. HP blev banebrydende inden for desktopadministration, da vi i 1995 lancerede branchens første pc med fuld understøttelse af desktopadministration. HP har patent på denne administrationsteknologi. Siden da er HP gået i front for at udvikle standarder og den infrastruktur, som kræves for at optimere anvendelsen, konfigurationen og håndteringen af skriveborde, arbejdsstationer og notebook-pc'er. HP arbejder tæt sammen med industriens førende producenter af administrationsprogrammer for at sikre kompatibilitet mellem Intelligent Manageability og disse produkter. Intelligent Administration er en vigtig del af vores arbejde med at udvikle komplette pc-løsninger, der hjælper dig gennem desktopcomputerens fire faser – planlægning, implementering, administration og opgradering.

De væsentligste faciliteter og funktioner i desktopadministration er:

- Førstegangskonfiguration og implementering
- Fjerninstallation
- Opdatering og administration af software
- ROM Flash
- Ressourceovervågning og -sikkerhed
- Fejlmeddelelser og genoprettelse

Visse funktioner, der er beskrevet her, understøttes kun af udvalgte computermodeller og softwareversioner.

Førstegangskonfiguration og implementering

Computeren leveres med forudinstalleret systemsoftware. I løbet af et øjeblik pakkes softwaren ud, og computeren er klar til brug.

Du kan vælge at udskifte den præinstallerede software med brugerdefineret system- og programsoftware. Du kan oprette brugerdefinerede softwareløsninger på flere måder. Blandt andet:

- Installere ekstra software efter udpakning af den præinstallerede software.
- Bruge softwareinstallationsværktøjer, f.eks. Altiris Deployment Solution™, til at erstatte den forudinstallerede software med brugerdefineret software.
- Kopiere indholdet fra én harddisk til en anden via diskkloning.

Det er din it-platform og -arbejdsprocesser, der afgør, hvilken implementeringsmetode der er den bedste. Du kan få hjælp til at vælge den bedste metode i afsnittet PC Deployment på hjemmesiden HP Lifecycle Solutions (http://h18000.www1.hp.com/solutions/pcsolutions).

Cd'en *Restore Plus!*, ROM-baseret opsætning og ACPI-hardware giver yderligere assistance ved genoprettelse af systemsoftware, konfigurationsstyring og fejlfinding samt strømstyring.

Fjerninstallation

Fjerninstallation giver mulighed for start og opsætning af systemet med de oplysninger om software og konfiguration, der findes på en netværksserver, ved at starte PXE (Preboot Execution Environment). Fjerninstallationen bruges oftest som et værktøj til systemopsætning og konfiguration og kan bruges til følgende opgaver:

- Formatering af en harddisk
- Implementering af systemsoftware på en eller flere nye pc'er
- Fjernopdatering af systemets BIOS i flash-ROM'en ("Ekstern ROM-hukommelsesflash" på side 7)
- Konfiguration af systemets BIOS-indstillinger

Tryk på **F12**, når der står F12 = Network Service Boot i nederste højre hjørne af HP-logoskærmen, for at aktivere fjerninstallationen. Følg vejledningen på skærmen for at fortsætte. Standardstartrækkefølgen er en konfigurationsindstilling i BIOS, der kan ændres til altid at forsøge at PXE-starte.

HP og Altiris, Inc. samarbejder om et værktøj, der er beregnet til at gøre udnyttelse og administration af pc'er i virksomheder nemmere og mindre tidskrævende og derved mindske totalomkostningerne ved ejerskab og gøre pc'er fra HP til de mest håndterbare klient-pc'er i virksomhedsmiljøer.

Opdatering og håndtering af software

HP tilbyder flere værktøjer til håndtering og opdatering af software på skriveborde og arbejdsstationer – Altiris; Altiris PC Transplant Pro; HP Client Manager Software, der er en Altiris-løsning, System Software Manager; Proactive Change Notification og ActiveUpdate.

HP Client Manager-software

Intelligent HP Client Manager Software (HP CMS) integrerer HP Intelligent Manageability-teknologien i Altiris med henblik på at tilbyde de bedste hardwarehåndteringsegenskaber til HP-enheder, herunder:

- Detaljeret visning af hardwarebeholdningen til ressourcestyring
- Overvågning og diagnosticering af pc'ens helbredstilstand
- Proaktiv besked i tilfælde af ændringer i hardwaremiljøet
- Rapportering af forretningskritiske oplysninger med webadgang, f.eks. oplysninger om overophedede maskiner, hukommelsesproblemer mm
- Fjernopdatering af systemsoftware, f.eks. enhedsdrivere og ROM BIOS
- Fjernændring af startrækkefølgen

Find flere oplysninger om HP Client Manager på http://h18000.www1.hp.com/im/client_mgr.html.

Altiris-løsninger

HP Client Management-løsninger giver centraliseret hardwareadministration af HP-klientenheder til alle it-livscyklusområder.

- Administration af aktiver og ressourcer
  - ❏ Softwarelicensoverensstemmelse
  - ❏ PC-sporing og rapportering
  - ❏ Lejeaftale, oprettelse af ressourcesporing
- Implementering og overflytning
  - ❏ Overflytning af Microsoft Windows 2000 eller Windows XP Professional eller Home Edition
  - ❏ Systemimplementering
  - ❏ Overflytning af personlige indstillinger

- HelpDesk og problemløsning
  - Håndtering af HelpDesk-spørgsmål
  - Fjernfejlfinding
  - Fjernproblemløsning
  - Gendannelse efter klientsammenbrud
- Administration af software og drift
  - Løbende desktopadministration
  - Softwareimplementering på HP-system
  - Automatisk programreparation

På udvalgte desktop- og bærbare modeller er en Altiris-administrationsagent inkluderet som en del af standardprogrammerne. Denne agent aktiverer kommunikation med Altiris-udviklingsløsningen, der kan benyttes til implementering af helt ny hardware eller overflytning af personlige indstillinger til et nyt operativsystem ved hjælp af brugervenlige guider. Altiris-løsningerne indeholder desuden faciliteter til nem distribution af software. Ved brug sammen med SSM (System Software Manager) eller HP Client Manager kan administratoren også opdatere ROM BIOS'en og softwaren til enhedsdriveren fra en central computer.

Yderligere oplysninger finder du på http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro sikrer en smertefri pc-overflytning, fordi gamle indstillinger, parametre og data hurtigt og nemt bevares og overflyttes til det nye miljø. Opgraderinger tager få minutter i modsætning til tidligere timer eller dage, og skrivebordet ser ud som og fungerer, som brugerne forventer det.

Yderligere oplysninger og detaljer om at downloade en fuldt funktionsdygtig 30-dages evalueringsversion finder du på http://h18000.www1.hp.com/im/prodinfo.html#deploy.

SSM (System Software Manager)

SSM (System Software Manager) er et program, der gør det muligt at opdatere software på systemniveau på flere systemer på én gang. Hvis SSM startes på et pc-klientsystem, registrerer programmet både hardware- og softwareversioner og opgraderer automatisk den relevante software fra en central base, også kaldet et filbibliotek. De driverversioner, der understøttes af SSM, er markeret med et specielt symbol på den hjemmeside, hvorfra drivere kan hentes, og på cd'en Support Software. Du kan hente hjælpeprogrammet eller få flere oplysninger om SSM på: http://h18000.www1.hp.com/im/ssmwp.html.

PCN (Product Change Notification)

Programmet PCN bruger det sikre websted Subscriber's Choice til proaktivt og automatisk at kunne:

- Sende dig PCN-e-mails med oplysninger om hardware- og softwareændringer af de fleste kommercielle computere og servere op til 60 dage forud.
- Sende dig e-mails med kundeoplysninger, kunderådgivning, kundebemærkninger, sikkerhedsbulletiner og driveralarmer til de fleste kommercielle computere og servere.

Opret din egen profil for at sikre, at du kun modtager de oplysninger, der er relevante for dit it-miljø. Yderligere oplysninger om programmet PCN (Proactive Change Notification) og om at oprette en brugerdefineret profil, finder du på http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate er et klientbaseret program fra HP. ActiveUpdate-klienten kører på det lokale system og anvender en brugerdefineret profil til proaktivt og automatisk at hente softwareopdateringer til de fleste af de HP-computere og -servere, der findes i handlen. Når du har hentet en softwareopdatering, implementeres den intelligent på de computere, den er beregnet til, af HP Client Manager-software og System Software Manager.

Yderligere oplysninger om ActiveUpdate, om at hente programmet og oprette en kundeprofil finder du på: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

ROM Flash

Computeren leveres med en programmerbar flash-ROM (Read Only Memory). ROM'en kan beskyttes mod utilsigtet opdatering eller overskrivning, hvis der oprettes en adgangskode for opsætning i hjælpeprogrammet Computer Setup (F10). Dette er vigtigt for at sikre computerens driftsikkerhed. Hvis du skal eller vil opgradere ROM'en, kan du gøre ét af følgende:

- Bestil en opgraderet ROMPaq-diskette fra HP.
- Hent den seneste ROMPaq-software fra http://h18000.www1.hp.com/im/ssmwp.html.

FORSIGTIG: Sørg for at oprette en adgangskode for opsætning for maksimal beskyttelse af ROM-hukommelsen. Adgangskoden for opsætning forhindrer uautoriserede opgraderinger af ROM-hukommelsen. System Software Manager gør det muligt for systemadministratoren at angive adgangskoden for opsætning på en eller flere pc'er samtidigt. Yderligere oplysninger finder du på http://h18000.www1.hp.com/im/ssmwp.html.

Ekstern ROM-hukommelsesflash

En ekstern ROM-hukommelsesflash giver systemadministratoren mulighed for at opgradere ROM-hukommelsen på eksterne HP-computere på en sikker måde direkte fra den centrale netværkskonsol. Når systemadministratoren kan udføre denne opgave eksternt på flere computere, opnås en ensartet implementering af og større kontrol over HP PC ROM-billeder over netværket. Dette giver også større produktivitet og lavere omkostninger ved at eje computerne.

Computeren skal tændes eller skal være tændt gennem Remote Wakeup for at kunne benytte Remote ROM Flash.

Yderligere oplysninger om Remote ROM Flash finder du under HP Client Manager Software eller System Software Manager på http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

Hjælpeprogrammet HPQFlash bruges til lokalt at opdatere eller gendanne systemets ROM på individuelle computere via et Windows-operativsystem.

Yderligere oplysninger om HPQFlash finder du på http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

FailSafe Boot Block ROM

FailSafe Boot Block ROM giver mulighed for genoprettelse af systemet, såfremt der opstår fejl under ROM-flash, f.eks. hvis der opstår et strømsvigt under en ROM-opgradering. Boot Block er en beskyttet del af ROM'en, der foretager kontrol for at validere systemets ROM, hver gang den aktiveres.

- Hvis systemets ROM er gyldig, starter systemet på normal vis.
- Hvis systemets ROM ikke findes gyldig, leverer FailSafe Boot Block ROM understøttelse til at starte systemet fra en ROMPaq-diskette, der programmerer systemets ROM med et gyldigt billede.

Når Boot Block finder en ugyldig systemhukommelse, blinker den røde lysdiode for strøm otte gange pr. sekund, efterfulgt af en pause på to sekunder. Der høres også otte samtidige bip. Der vises en meddelelse om Boot Block-gendannelse på skærmen (udvalgte modeller).

Følg fremgangsmåden nedenfor for at genoprette systemet, når Boot Block-funktionen er aktiveret:

1. Hvis der er sat en diskette i diskettedrevet, skal du fjerne den og slukke for strømmen.
2. Sæt en ROMPaq-diskette i diskettedrevet.
3. Tænd systemet.
4. Hvis der ikke findes en ROMPaq-diskette, bliver du bedt om at isætte en og genstarte computeren.
5. Hvis der er oprettet en adgangskode for opsætning, tænder Caps Lock, og du bliver bedt om at angive adgangskoden.

6. Angiv adgangskoden for opsætning.
7. Hvis systemet startes fra disketten og genprogrammerer ROM-hukommelsen, vil de tre lysdioder på tastaturet lyse. En serie bip af stigende styrke signalerer desuden vellykket udførsel.
8. Fjern disketten, og sluk for strømmen.
9. Tænd for strømmen igen for at genstarte computeren.

Tabellen nedenfor viser de forskellige tastaturlyskombinationer, som bruges af Boot Block ROM (når der er tilsluttet et PS/2-tastatur til computeren) og forklarer den betydning og handling, der er tilknyttet hver kombination.

Kombinationer af lysdioder på tastaturer under Boot Block ROM

FailSafe Boot Block-tilstand	Farve på lysdiode for tastatur	Tastatur Lysdiodeaktivitet	Tilstand/meddelelse
Num Lock	Grøn	Tændt	ROMPaq-disketten mangler, er beskadiget, eller drevet er ikke klart.
Caps Lock	Grøn	Tændt	Angiv adgangskode.
Num, Caps, Scroll Lock	Grøn	Blinker i sekvens, en ad gangen – N, C, SL	Tastatur låst i netværkstilstand.
Num, Caps, Scroll Lock	Grøn	Tændt	Gennemført Boot Block ROM Flash. Sluk for strømmen, og tænd igen for at genstarte.

✎ Lysdioder for diagnosticering blinker ikke på USB-tastaturer.

Replikering af opsætningen

Følgende fremgangsmåder giver administratoren mulighed for nemt at kopiere en opsætningskonfiguration til andre computere af samme model. Dette giver hurtigere og mere konsekvent konfiguration af flere computere.

Til begge fremgangsmåder kræves et diskettedrev eller en understøttet USB-flashmedieenhed, f.eks. HP Drive Key.

Kopiering til en enkelt computer

FORSIGTIG: En konfiguration af opsætningen gælder for den enkelte model. Filsystemet kan blive ødelagt, hvis kilde- og destinationscomputerne ikke er af samme model. Du skal f.eks. ikke kopiere opsætningskonfigurationen fra en D510 US-desktop til en D510 e-pc.

1. Vælg den opsætningskonfiguration, der skal kopieres. Tænd, eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Sæt en diskette eller en USB-flashmedieenhed i computeren.
4. Klik på **File > Save to Diskette**. Følg anvisningerne på skærmen for at oprette konfigurationsdisketten eller USB-flashmedieenheden.
5. Sluk den computer, der skal konfigureres, og sæt konfigurationsdisketten eller USB-flashmedieenheden i.
6. Tænd den computer, der skal konfigureres. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.
7. Klik på **File > Restore from Diskette**, og følg vejledningen på skærmen.
8. Genstart computeren, når konfigurationen er fuldført.

Kopiering til flere computere

FORSIGTIG: En konfiguration af opsætningen gælder for den enkelte model. Filsystemet kan blive ødelagt, hvis kilde- og destinationscomputerne ikke er af samme model. Du skal f.eks. ikke kopiere opsætningskonfigurationen fra en D510 US-desktop til en D510 e-pc.

Denne fremgangsmåde kræver lidt mere tid til at forberede konfigurationsdisketten eller USB-flashmedieenheden, men en kopiering af konfigurationen til destinationscomputere er betydeligt hurtigere.

En diskette, computeren kan startes fra, kan ikke oprettes i Windows 2000. Der kræves en diskette, computeren kan startes fra, til denne fremgangsmåde eller for at oprette en USB-flashmedieenhed, computeren kan startes fra. Hvis Windows 9x eller Windows XP ikke kan bruges til at oprette en startdiskette, kan du benytte metoden til at kopiere til en enkelt computer i stedet for (se "Kopiering til en enkelt computer" på side 10).

1. Opret en startdiskette eller en USB flashmedieenhed. Se "Startdiskette" på side 12, "Understøttet USB-flashmedieenhed" på side 13 eller "Ikke-understøttet USB-flashmedieenhed" på side 16.

FORSIGTIG: Ikke alle computere kan startes fra en USB-flashmedieenhed. Hvis standardstartrækkefølgen i hjælpeprogrammet Computer Setup (F10) viser USB-enheden før harddisken, kan computeren startes fra en USB-flashmedieenhed. Ellers skal der bruges en startdiskette.

2. Vælg den opsætningskonfiguration, der skal kopieres. Tænd, eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
3. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

4. Sæt startdisketten eller USB-flashmedieenheden i computeren.
5. Klik på **File > Save to Diskette**. Følg anvisningerne på skærmen for at oprette konfigurationsdisketten eller USB-flashmedieenheden.
6. Hent et BIOS-hjælpeprogram til at replikere opsætningen (repset.exe), og kopier det til konfigurationsdisketten eller USB-flashmedieenheden. Hjælpeprogrammet kan hentes på http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Opret en autoexec.bat-fil på konfigurationsdisketten eller USB-flashmedieenheden med følgende kommando:

   repset.exe

8. Sluk den computer, der skal konfigureres. Sæt konfigurationsdisketten eller USB-flashmedieenheden i computeren, og tænd computeren. Konfigurationshjælpeprogrammet kører automatisk.
9. Genstart computeren, når konfigurationen er komplet.

Oprettelse af en startenhed

Startdiskette

Disse instruktioner gælder for Windows XP Professional og Home Edition. Windows 2000 understøtter ikke oprettelsen af en startdiskette.

1. Indsæt en diskette i diskettedrevet.
2. Klik på **Start** og derefter **Denne computer**.
3. Højreklik på diskettedrevet, og klik derefter på **Formater**.
4. Marker afkrydsningsfeltet **Opret en MS-DOS-startdiskette**, og klik derefter på **Start**.

Gå tilbage til "Kopiering til flere computere" på side 11.

Understøttet USB-flashmedieenhed

Understøttede enheder, f.eks. HP Drive Key eller DiskOnKey, har forudinstalleret software, som gør det lettere at oprette startenheder. Hvis den Drive Key, der benyttes, ikke indeholder denne software, skal du benytte den fremgangsmåde, der er beskrevet senere i afsnittet (se "Ikke-understøttet USB-flashmedieenhed" på side 16).

FORSIGTIG: Ikke alle computere kan startes fra en USB-flashmedieenhed. Hvis standardstartrækkefølgen i hjælpeprogrammet Computer Setup (F10) viser USB-enheden før harddisken, kan computeren startes fra en USB-flashmedieenhed. Ellers skal der bruges en startdiskette.

Der kræves følgende, for at du kan oprette en USB-flashmedieenhed som startenhed:

- Et af følgende systemer:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 konvertibelt minitower/SFF
  - HP Compaq Business Desktop d530-serien – Ultra-slim desktop, SFF eller konvertibelt minitower
  - Bærbare modeller Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c
  - Bærbare modeller Compaq Presario 1500 eller 2800

  Afhængigt af den enkelte BIOS kan fremtidige systemer også understøtte start via HP Drive Key.

FORSIGTIG: Hvis din computer ikke er nævnt herover, skal du kontrollere, at standardstartrækkefølgen i hjælpeprogrammet Computer Setup (F10) viser USB-enheden før harddisken.

- Et af følgende datalagringsmoduler:
  - 16 MB HP Drive Key
  - 32 MB HP Drive Key
  - 32 MB DiskOnKey
  - 64 MB HP Drive Key
  - 64 MB DiskOnKey
  - 128 MB HP Drive Key
  - 128 MB DiskOnKey

- En DOS-startdiskette med programmerne FDISK og SYS. Hvis SYS ikke er tilgængelig, kan FORMAT benyttes, men alle eksisterende filer på Drive Key går tabt.

1. Sluk computeren.
2. Sæt Drive Key i en af computerens USB-porte, og afbryd alle andre USB-datalagringsenheder undtagen USB-diskettedrevene.
3. Sæt en DOS-startdiskette med FDISK.COM og enten SYS.COM eller FORMAT.COM i et diskettedrev, og tænd computeren for at starte fra DOS-disketten.
4. Kør FDISK fra A:\-prompten ved at skrive **FDISK** og trykke på Enter. Klik på **Yes** (**Y**), hvis du bliver bedt om det, for at aktivere understøttelse af en stor disk.
5. Indtast dit valg [**5**] for at få vist systemets drev. Drive Key vil være det drev, der bedst svarer til størrelsen på et af de angivne drev. Det er normalt det sidste drev på listen. Bemærk drevets bogstav.

   Drive Key-drev: _____

FORSIGTIG: Hvis drevet ikke passer til Drive Key, bør du ikke fortsætte. Du risikerer at miste data. Kontroller alle USB-porte for yderligere datalagringsenheder. Hvis du finder nogen, skal du fjerne dem, genstarte computeren, og gå videre fra trin 4. Hvis du ikke finder nogen, understøtter systemet enten ikke Drive Key, eller Drive Key-enheden er defekt. FORTSÆT IKKE med at gøre Drive Key til startenhed.

6. Afslut FDISK ved at trykke på **Esc-tasten** for at vende tilbage til A:\-prompten.
7. Hvis DOS-startdisketten indeholder SYS.COM, skal du gå videre til trin 8. Ellers gå til trin 9.
8. Indtast kommandoen **SYS x:** ved A:\-prompten. Her repræsenterer x det drevbogstav, du har noteret tidligere. Gå til trin 13.

FORSIGTIG: Kontroller, at du har indtastet det rigtige drevbogstav for Drive Key.

Når systemfilerne er blevet overflyttet, vender SYS tilbage til A:\-prompten.

9. Kopier de filer, du vil beholde, fra Drive Key til en temporær mappe på et andet drev, f.eks. systemets interne harddisk.
10. Indtast kommandoen **FORMAT /S X:** ved A:\-prompten. Her repræsenterer x det drevbogstav, du har noteret tidligere.

FORSIGTIG: Kontroller, at du har indtastet det rigtige drevbogstav for Drive Key.

FORMAT viser en eller flere advarsler og spørger dig hver gang, om du vil fortsætte. Skriv **y** hver gang. FORMAT formaterer nu Drive Key, tilføjer systemfiler og beder dig angive et enhedsnavn.

11. Tryk på **Enter**, hvis du ikke vil angive et enhedsnavn, eller skriv det ønskede navn.
12. Kopier de filer, du eventuelt gemte under trin 9, tilbage til Drive Key.
13. Tag disketten ud, og genstart computeren. Computeren starter op med Drive Key som C-drev.

Standardstartrækkefølgen varierer fra computer til computer, og den kan ændres i hjælpeprogrammet Computer Setup (F10).

Hvis du har brugt en DOS-version fra Windows 9x, kan du kort se en side med Windows-logoet. Hvis du ikke vil se denne side, kan du tilføje en fil af længden nul med navnet LOGO.SYS i rodmappen på Drive Key.

Gå tilbage til "Kopiering til flere computere" på side 11.

Ikke-understøttet USB-flashmedieenhed

FORSIGTIG: Ikke alle computere kan startes fra en USB-flashmedieenhed. Hvis standardstartrækkefølgen i hjælpeprogrammet Computer Setup (F10) viser USB-enheden før harddisken, kan computeren startes fra en USB-flashmedieenhed. Ellers skal der bruges en startdiskette.

Der kræves følgende, for at du kan oprette en USB-flashmedieenhed som startenhed:

- Et af følgende systemer:
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 konvertibelt minitower/SFF
  - HP Compaq Business Desktop d530-serien – Ultra-slim desktop, SFF eller konvertibelt minitower
  - Bærbare modeller Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c eller N1000c
  - Bærbare modeller Compaq Presario 1500 eller 2800

  Afhængigt af den enkelte BIOS kan fremtidige systemer også understøtte start via en USB-flashmedieenhed.

FORSIGTIG: Hvis din computer ikke er nævnt herover, skal du kontrollere, at standardstartrækkefølgen i hjælpeprogrammet Computer Setup (F10) viser USB-enheden før harddisken.

- En DOS-startdiskette med programmerne FDISK og SYS. Hvis SYS ikke er tilgængelig, kan FORMAT benyttes, men alle eksisterende filer på Drive Key går tabt.

1. Hvis systemet indeholder PCI-kort med et drev af typen SCSI, ATA RAID eller SATA tilknyttet, skal du slukke computeren og tage netledningen ud.

FORSIGTIG: Netledningen SKAL tages ud af computeren.

2. Åbn computeren, og tag PCI-kortene ud.
3. Sæt USB-flashmedieenheden i en af computerens USB-porte, og afbryd alle andre USB-datalagringsenheder undtagen USB-diskettedrevene. Luk computerens låg.
4. Sæt netledningen i, og tænd computeren. Så snart lysdioden på skærmen lyser grønt, skal du trykke på tasten **F10** for at gå ind i computerens opsætningsprogram.
5. Gå til Advanced/PCI devices for at deaktivere både IDE- og SATA-controllerne. Når du deaktiverer SATA-controlleren, skal du bemærke den IRQ, som controlleren er tildelt. Du skal tildele IRQ'en igen senere. Afslut opsætningen, og godkend ændringerne.

   SATA IRQ: _____
6. Sæt en DOS-startdiskette med FDISK.COM og enten SYS.COM eller FORMAT.COM i et diskettedrev, og tænd computeren for at starte fra DOS-disketten.
7. Kør FDISK, og slet eventuelle eksisterende diskpartitioner på USB-flashmedieenheden. Opret en ny partition, og marker den som aktiv. Afslut FDISK ved at trykke på **Esc**-tasten.
8. Hvis systemet ikke automatisk genstarter, når du afslutter FDISK, skal du trykke på **Ctrl+Alt+Del** for at genstarte fra DOS-disketten.
9. Indtast ved A:\-prompten kommandoen **FORMAT C: /S**, og tryk på **Enter**. FORMAT formaterer nu USB-flashmedieenheden, tilføjer systemfilerne og beder dig angive et enhedsnavn.
10. Tryk på **Enter**, hvis du ikke vil angive et enhedsnavn, eller skriv det ønskede navn.
11. Sluk computeren, og tag netledningen ud. Åbn computeren, og installer de PCI-kort igen, som du eventuelt tog ud tidligere. Luk computerens låg.
12. Sæt netledningen i, tag disketten ud, og tænd computeren.
13. Så snart lysdioden på skærmen lyser grønt, skal du trykke på tasten **F10** for at gå ind i computerens opsætningsprogram.

14. Gå til Advanced/PCI Devices, og aktiver de IDE- og SATA-controllere, der blev deaktiverede under trin 5. Indstil SATA-controlleren på den oprindelige IRQ.
15. Gem ændringerne, og afslut. Computeren starter op via USB-flashmedieenheden som C-drev.

Standardstartrækkefølgen varierer fra computer til computer, og den kan ændres i hjælpeprogrammet Computer Setup (F10).

Hvis du har brugt en DOS-version fra Windows 9x, kan du kort se en side med Windows-logoet. Hvis du ikke vil se denne side, kan du tilføje en fil af længden nul med navnet LOGO.SYS i rodmappen på Drive Key.

Gå tilbage til "Kopiering til flere computere" på side 11.

Tovejs afbryderknap

Med Advanced Configuration and Power Interface (ACPI) aktiveret til Windows 2000 og Windows XP Professional og Home Edition kan afbryderknappen fungere både som en tænd/sluk-knap og som en pauseknap. Pausefunktionen slukker ikke strømmen helt, men får i stedet computeren til at gå i venteposition med et lavt strømforbrug. Dette giver dig mulighed for hurtigt at lukke ned uden at lukke selve programmerne og hurtigt at komme tilbage til samme driftstilstand uden tab af data.

Følg fremgangsmåden nedenfor for at ændre afbryderknappens konfiguration:

1. Venstreklik i Windows 2000 på **knappen Start**, og marker derefter **Indstillinger > Kontrolpanel > Strømstyring**.

   Venstreklik i Windows XP Professional og Home Edition på **knappen Start**, og marker derefter **Kontrolpanel > Ydelse og vedligeholdelse > Strømstyring**.

2. Marker fanen **Avanceret** under egenskaberne for **Strømstyring**.
3. Marker den ønskede indstilling for afbryderen i afsnittet **Afbryderknapper**.

Efter konfiguration af afbryderknappen til at fungere som en pauseknap skal du trykke på afbryderknappen for at indstille systemet til strømsparetilstand (pause). Tryk på knappen igen for hurtigt at bringe systemet ud af pausetilstand til fuld spænding. Tryk på afbryderknappen, og hold den nede i fire sekunder for helt at slukke computeren.

FORSIGTIG: Undgå at bruge afbryderen til at slukke computeren, medmindre systemet ikke reagerer. Når du slukker systemet uden om operativsystemet, kan data på harddisken blive beskadiget eller gå tabt.

Hjemmeside

HP's ingeniører tester og udfører fejlfinding på software, der udvikles af HP og andre tredjepartsleverandører, samt udvikler operativsystemspecifik supportsoftware for at sikre HP-pc'ernes høje ydeevne, kompatibilitet og stabilitet.

Når der skiftes til et nyere eller et opdateret operativsystem, er det vigtigt at implementere de hjælpeprogrammer, der er udviklet til netop dette operativsystem. Hvis du planlægger at køre en version af Microsoft Windows, der er anderledes end den version, der følger med computeren, skal du installere de tilsvarende enhedsdrivere og hjælpeprogrammer for at sikre, at alle funktioner understøttes og fungerer korrekt.

HP har gjort det nemmere at finde, få adgang til, evaluere og installere de nyeste programmer. Du kan hente softwaren på http://www.hp.com/support.

Hjemmesiden indeholder de nyeste enhedsdrivere, hjælpeprogrammer og ROM-billeder, der kan flashes, som er nødvendige for at køre det nyeste Microsoft Windows-operativsystem på HP-computeren.

Moduler og partnere

HP-administrationsløsninger kan integreres i andre systemadministrationsprogrammer og er baseret på industristandarder, f.eks.:

- DMI 2.0 (Desktop Management Interface)
- Wake on LAN-teknologi
- ACPI
- SMBIOS
- PXE-support (Pre-boot Execution)

Ressourceovervågning og sikkerhed

Ressourceovervågningsfunktionerne i computeren tilbyder vigtige data, der kan håndteres ved hjælp af HP Insight Manager, HP Client Manager eller andre systemadministrationsprogrammer. Nem, automatisk integration mellem ressourceovervågningsfunktionerne og disse produkter gør det muligt at vælge det administrationsværktøj, der passer bedst til miljøet, og udnytte investeringen i eksisterende værktøjer bedst muligt.

HP tilbyder også flere løsninger til kontrol af adgangen til værdifulde computerkomponenter og -oplysninger. ProtectTools Embedded Security forhindrer, hvis det er installeret, uautoriseret adgang til data og kontrollerer systemets integritet og godkender tredjepartsbrugere, der forsøger at få adgang til systemet. Sikkerhedsfunktioner, f.eks. beskyttelsesværktøjerne Smart Cover Sensor og Smart Cover Lock, som findes på udvalgte modeller, skal medvirke til at forhindre uautoriseret adgang til computerens interne komponenter. Ved at deaktivere USB-portene, de parallelle eller serielle porte, eller ved at deaktivere muligheden for opstart fra flytbare medier kan du beskytte vigtige data. Med Memory Change og Smart Cover Sensor kan der automatisk sendes advarsler til systemadministrationsprogrammer for give proaktiv besked om forsøg på at få adgang til computerens interne komponenter.

Beskyttelsesværktøjerne Smart Cover Sensor og Smart Cover Lock findes som ekstraudstyr på udvalgte systemer.

Brug følgende hjælpeprogrammer til at redigere sikkerhedsindstillingerne på HP-computeren:

- Lokalt ved hjælp af funktionerne i Computer Setup. Se vejledningen til hjælpeprogrammet *Computer Setup (F10)*, der fulgte med computeren, for at få flere oplysninger om at bruge hjælpeprogrammerne.
- Som fjernbruger ved hjælp af HP Client Manager eller System Software Manager. Denne software muliggør sikker, ensartet implementering og styring af indstillinger for sikkerhed via kommandolinjen i et enkelt program.

Nedenstående tabel og afsnit henviser til lokal håndtering af computerens sikkerhedsfunktioner via hjælpeprogrammet Computer Setup (F10).

Oversigt over sikkerhedsfunktioner

Funktion	Formål	Oplysninger om oprettelse
Removable Media Boot Control	Forhindrer opstart fra løse mediedrev. (tilgængelig på udvalgte drev).	I menuen i hjælpeprogrammet Computer Setup (F10).
Serial, Parallel, USB, or Infrared Interface Control	Forhindrer overførsel af data gennem den integrerede serielle, parallelle, USB- (Universel Seriel Bus) eller infrarøde brugergrænseflade.	I menuen i hjælpeprogrammet Computer Setup (F10).
Power-On Password	Forhindrer brug af computeren, indtil adgangskoden angives. Dette kan gælde både for første opstart og genstart af systemet.	I menuen i hjælpeprogrammet Computer Setup (F10).
Setup Password	Forhindrer rekonfiguration af computeren (brug af hjælpeprogrammet Computeropsætning), indtil adgangskoden angives.	I menuen i hjælpeprogrammet Computer Setup (F10).
Embedded Security Device	Forhindrer uautoriseret adgang til data ved hjælp af kryptering og beskyttelse med adgangskode. Kontrollerer systemets integritet og godkender tredjepartsbrugere, som forsøger at få adgang til systemet.	I menuen i hjælpeprogrammet Computer Setup (F10).

✎ Yderligere oplysninger om computerens opsætning finder du i vejledningen til hjælpeprogrammet *Computer Setup (F10)*.

Understøttelsen af sikkerhedsfunktionerne varierer afhængigt af computerens specifikke konfiguration.

Oversigt over sikkerhedsfunktioner *(Fortsat)*

Funktion	Formål	Oplysninger om oprettelse
DriveLock	Forhindrer uautoriseret adgang til data på MultiBay-harddiske. Denne funktion er standard på udvalgte modeller.	I menuen i hjælpeprogrammet Computer Setup (F10).
Smart Cover Sensor	Angiver, at et dæksel eller sidepanel er fjernet. Kan indstilles til at kræve adgangskoden for opsætning før genstart af computeren, når dækpladen eller sidepanelet har været fjernet. Se *Hardwarevejledning* på cd'en *Documentation Library* for at få flere oplysninger. Denne funktion er standard på udvalgte modeller.	I menuen i hjælpeprogrammet Computer Setup (F10).
Master Boot Record Security	Kan forhindre utilsigtet eller fjendtlige ændringer af MBR (Master Boot Record) på den aktuelle startdisk og kan genoprette den "seneste fungerende" MBR.	I menuen i hjælpeprogrammet Computer Setup (F10).
Memory Change Alerts	Identificerer tilføjelser, flytning eller fjernelse af hukommelsesmoduler og advarer slutbruger og systemadministrator.	Se i onlinevejledningen om *intelligent administration* for at få flere oplysninger om aktivering af advarsler om hukommelsesændringer.

✎ Yderligere oplysninger om computerens opsætning finder du i vejledningen til hjælpeprogrammet *Computer Setup (F10)*.

Understøttelsen af sikkerhedsfunktionerne varierer afhængigt af computerens specifikke konfiguration.

Oversigt over sikkerhedsfunktioner *(Fortsat)*

Funktion	Formål	Oplysninger om oprettelse
Ownership Tag	Viser oplysninger om ejeren, som defineret af systemadministratoren, under systemstart (beskyttet af adgangskode for opsætning).	I menuen i hjælpeprogrammet Computer Setup (F10).
Cable Lock Provision	Spærrer adgang til den interne del af computeren for at forhindre uønskede konfigurationsændringer eller fjernelse af komponenter. Kan også bruges til at fastgøre computeren til en fast genstand for at forhindre tyveri.	Monter en kabellås for at fastgøre computeren til en fast genstand.
Security Loop Provision	Spærrer adgang til den interne del af computeren for at forhindre uønskede konfigurationsændringer eller fjernelse af komponenter.	Sæt en lås i sikkerhedsløkken for at forhindre uønskede ændringer af konfigurationen, eller at der fjernes komponenter.

✎ Yderligere oplysninger om computerens opsætning finder du i vejledningen til hjælpeprogrammet *Computer Setup (F10)*.

Understøttelsen af sikkerhedsfunktionerne varierer afhængigt af computerens specifikke konfiguration.

Sikkerhed med adgangskode

Adgangskoden for opstart forhindrer uautoriseret brug af computeren ved at kræve, at der angives en adgangskode for at få adgang til programmer og data, hver gang computeren startes. Adgangskoden for opsætning forhindrer uautoriseret adgang til programmet Computer Setup og kan også anvendes til at tilsidesætte adgangskoden for opstart. Det betyder, at du kan angive adgangskoden for opsætning i stedet for adgangskoden for start i indtastningsfeltet for at få adgang til computeren.

Det er ligeledes muligt at oprette en adgangskode, der gælder i hele netværket, og som gør det muligt for systemadministratoren at logge ind på alle netværkssystemer uden at skulle kende adgangskoden for opstart.

Angivelse af opsætningsadgangskode ved hjælp af programmet Computer Setup

Hvis systemet er udstyret med en integreret sikkerhedsenhed, henvises til "Embedded Security" på side 30.

Angivelse af en adgangskode for opsætning gennem Computer Setup forhindrer, at computerens konfiguration ændres (brug af hjælpeprogrammet Computer Setup (F10)), indtil adgangskoden indtastes.

1. Tænd, eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security**, vælg **Setup Password**, og følg derefter instruktionerne på skærmen.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Oprettelse af en adgangskode for start ved hjælp af Computer Setup

Angivelse af en adgangskode for start i hjælpeprogrammet Computer Setup forhindrer adgang til computeren, når den er tændt, medmindre adgangskoden angives. Når der er angivet en adgangskode for start, vises indstillingerne for adgangskoden i menuen Security i Computer Setup. Indstillinger for adgangskode omfatter Password Prompt on Warm Boot. Hvis Password Prompt on Warm Boot er aktiveret, skal adgangskoden også angives, hver gang computeren genstartes.

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security**, vælg **Power-On Password**, og følg derefter instruktionerne på skærmen.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Angivelse af en adgangskode for start

Følg fremgangsmåden nedenfor for at angive en adgangskode for start:

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Angiv den aktuelle adgangskode, når nøgleikonet vises på skærmen, og tryk på **Enter**.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

Hvis du angiver en forkert adgangskode, vises et ikon med en overkrydset nøgle. Forsøg igen. Du skal slukke og tænde computeren igen, før du kan fortsætte, hvis du skriver forkert tre gange.

Angivelse af adgangskode for opsætning

Hvis systemet er udstyret med en integreret sikkerhedsenhed, henvises til "Embedded Security" på side 30.

Hvis der er angivet en adgangskode for opsætning på computeren, vil du blive bedt om at indtaste den, hver gang du kører programmet Computer Setup.

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Angiv adgangskoden for opsætning, når nøgleikonet vises på skærmen, og tryk på **Enter**.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

Hvis du angiver en forkert adgangskode, vises et ikon med en overkrydset nøgle. Forsøg igen. Du skal slukke og tænde computeren igen, før du kan fortsætte, hvis du skriver forkert tre gange.

Ændring af adgangskode for start eller opsætning

Hvis systemet er udstyret med en integreret sikkerhedsenhed, henvises til "Embedded Security" på side 30.

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows. Kør **Computer Setup** for at ændre adgangskoden for opsætning.
2. Skriv den aktuelle adgangskode efterfulgt af en skråstreg (/) eller et andet afgrænsningstegn. Skriv den nye adgangskode efterfulgt af en skråstreg (/) eller et andet afgrænsningstegn, og skriv derefter den nye adgangskode igen som vist nedenfor, når nøgleikonet vises: **aktuel adgangskode/ny adgangskode/ny adgangskode**

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

3. Tryk på **Enter**.

Den nye adgangskode træder i kraft, næste gang du tænder computeren.

Oplysninger om andre afgrænsningstegn finder du i "Afgrænsningstegn for nationale tastaturer" på side 29. Adgangskoderne for start og opsætning kan også ændres under indstillingerne Security i programmet Computer Setup.

Sletning af adgangskode for start og opsætning

Hvis systemet er udstyret med en integreret sikkerhedsenhed, henvises til "Embedded Security" på side 30.

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows. Kør **Computer Setup** for at slette adgangskoden for opsætning.
2. Skriv den aktuelle adgangskode efterfulgt af en skråstreg (/) eller et andet afgrænsningstegn som vist herunder, når nøgleikonet vises: **aktuel adgangskode/**
3. Tryk på **Enter**.

Oplysninger om andre afgrænsningstegn finder du i "Afgrænsningstegn for nationale tastaturer". Adgangskoderne for start og opsætning kan også ændres under indstillingerne Security i programmet Computer Setup.

Afgrænsningstegn for nationale tastaturer

Hvert tastatur er konstrueret til at opfylde bestemte landes krav. Den syntaks og de taster, der anvendes til ændring eller sletning af adgangskoden afhænger af, hvilket tastatur der er leveret med computeren.

Afgrænsningstegn for nationale tastaturer

Arabisk	/	Græsk	-	Russisk	/
Belgisk	=	Hebraisk	.	Slovakisk	-
BHCSY*	-	Ungarsk	-	Spansk	-
Brasiliansk	/	Italiensk	-	Svensk/finsk	/
Kinesisk	/	Japansk	/	Schweizisk	-
Tjekkisk	-	Koreansk	/	Taiwansk	/
Dansk	-	Latinamerikansk	-	Thai	/
Fransk	!	Norsk	-	Tyrkisk	.
Fransk-canadisk	é	Polsk	-	Engelsk (Storbritannien)	/
Tysk	-	Portugisisk	-	Engelsk (USA)	/

* For Bosnien, Hercegovina, Kroatien, Slovenien og Jugoslavien

Fjernelse af adgangskode

Hvis du glemmer adgangskoden, gives der ikke adgang til computeren. Se *Vejledning til fejlfinding* for at få vejledning i fjernelse af adgangskoder.

Hvis systemet er udstyret med en integreret sikkerhedsenhed, henvises til "Embedded Security."

Embedded Security

Beskyttelsesværktøjet Embedded Security kombinerer kryptering og beskyttelse med adgangskode for at forbedre sikkerheden ved kryptering af EFS-filer/mapper (Embedded File System) og sikre e-mails med Microsoft Outlook og Outlook Express. ProtectTools findes til udvalgte professionelle desktopmodeller som CTO-tilbehør (Configured-To-Order). Det er beregnet til HP-kunder, for hvem datasikkerhed er af overordnet betydning. Uautoriseret adgang til data udgør en meget større fare end tab af data. ProtectTools anvender fire adgangskoder:

- (F10) Setup – Åbn hjælpeprogrammet Computer Setup (F10), og aktiver/deaktiver ProtectTools
- Take Ownership – Indstilles og bruges af systemadministratoren, som godkender brugerne og indstiller sikkerhedsparametrene
- Emergency Recovery Token – Indstilles af systemadministratoren og bruges til systemgendannelse ved fejl på computeren eller en ProtectTools-chip
- Basic User – Indstilles og anvendes af slutbrugeren.

Hvis slutbrugeren mister sin adgangskode, kan de krypterede data ikke gendannes. Derfor er det sikrest at bruge ProtectTools, når dataene på brugerens harddisk replikeres på systemets informationssystem eller sikkerhedskopieres regelmæssigt.

ProtectTools Embedded Security er en TCPA 1.1-kompatibel sikkerhedschip, der kan installeres på systemkortet som tilbehør på udvalgte professionelle desktopmodeller. Alle ProtectTools Embedded Security-chips er unikke og tilknyttet en bestemt computer. Chippen kører kernesikkerhedsprocesser uafhængigt af andre computerkomponenter, f.eks. processoren, hukommelsen eller operativsystemet.

En ProtectTools Embedded Security-aktiveret computer supplerer og forbedrer sikkerhedsfunktionerne i Microsoft Windows 2000 eller Windows XP Professional eller Home Edition. Operativsystemet kan f.eks. kryptere lokale filer og mapper baseret på EFS, men ProtectTools Embedded Security tilbyder et ekstra sikkerhedslag ved at oprette krypteringsnøgler ud fra platformens rodnøgle, der gemmes i silicium. Denne proces kaldes "wrapping" af krypteringsnøglerne. ProtectTools forhindrer ikke netværkets adgang til en computer uden ProtectTools.

De væsentligste funktioner i ProtectTools Embedded Security omfatter:

- Platformgodkendelse
- Beskyttet datalagring
- Dataintegritet

FORSIGTIG: Sikkerhedskopiering af adgangskoder. **Krypterede data kan ikke læses eller gendannes uden de rigtige adgangskoder**.

Opsætning af adgangskoder

Opsætning

Der kan oprettes en adgangskode til opsætning, og den integrerede sikkerhedsenhed kan aktiveres med hjælpeprogrammet Computer Setup F10.

1. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

2. Tryk på en af piletasterne (Pil op eller Pil ned), og vælg et sprog. Tryk herefter på **Enter**.
3. Klik på den venstre eller højre piletast for at flytte til fanen **Security**, og benyt derefter Pil op eller Pil ned til at flytte til **Setup Password**. Tryk på **Enter**.

4. Skriv en adgangskode, og godkend den. Tryk på **F10** for at godkende adgangskoden.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

5. Tryk på en af piletasterne (Pil op eller Pil ned) for at flytte til **Embedded Security Device**. Tryk på **Enter**.
6. Hvis markeringen i dialogboksen er **Embedded Security Device – Disable**, skal du bruge venstre eller højre piletast til at ændre den til **Embedded Security Device – Enable**. Tryk på **F10** for at godkende ændringen.

FORSIGTIG: Hvis du vælger **Reset to Factory Settings – Reset**, slettes indholdet af alle nøgler, og krypterede data vil ikke kunne gendannes, *medmindre* nøglerne er sikkerhedskopierede (se "Take Ownership og Emergency Recovery Token"). Vælg kun **Reset**, når du bliver bedt om at gøre det i fremgangsmåden til gendannelse af krypterede data (se "Gendannelse af krypterede data" på side 35).

7. Tryk på venstre eller højre piletast for at flytte til **File**. Tryk på Pil op eller Pil ned for at flytte til **Save Changes and Exit**. Tryk på **Enter**, og tryk derefter på **F10** for at godkende.

Take Ownership og Emergency Recovery Token

Take Ownership-adgangskoden skal indtastes for at aktivere eller deaktivere sikkerhedsplatformen og godkende brugere. Hvis den indbyggede sikkerhedsanordning ikke virker, kan brugerne ved hjælp af mekanismen Emergency Recovery blive godkendt og få adgang til data.

1. Hvis du kører Windows XP Professional eller Home Edition, skal du klikke på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

   Hvis du kører Windows 2000, skal du klikke på **Start > Programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Klik på **Next**.

3. Skriv og godkend en Take Ownership-adgangskode, og klik derefter på **Next**.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

4. Klik på **Next** for at acceptere standardplaceringen for gendannede arkiver.
5. Skriv og godkend en Emergency Recovery Token-adgangskode, og klik derefter på **Next**.
6. Sæt en diskette i, hvor du kan gemme Emergency Recovery Token Key. Klik på **Browse**, og vælg disketten.

FORSIGTIG: Emergency Recovery Token Key bruges til at gendanne krypterede data, hvis computeren eller den indbyggede sikkerhedschip ikke virker. **Dataene kan ikke gendannes uden nøglen**. Dataene kan ikke læses uden adgangskoden til basisbrugeren. Gem disketten på et sikkert sted.

7. Klik på **Save** for at godkende placeringen og standardfilnavnet, og klik derefter på **Next**.
8. Klik på **Next** for at godkende indstillingerne, før sikkerhedsplatformen initialiseres.

En meddelelse om, at de indbyggede sikkerhedsfunktioner ikke er initialiserede, vises muligvis. Klik ikke i meddelelsen. Den behandles senere i fremgangsmåden og lukker igen efter et par sekunder.

9. Klik på **Next** for at undgå konfiguration af lokale politikker.
10. Kontroller, at afkrydsningsfeltet Start Embedded Security User Initialization Wizard er markeret, og klik derefter på **Finish**.

Guiden User Initialization startes nu automatisk.

Basisbruger

Under brugerinitialiseringen oprettes en adgangskode til basisbrugeren. Denne adgangskode skal indtastes for at få adgang til krypterede data.

FORSIGTIG: Sikkerhedskopiering af basisbrugerens adgangskode. **Krypterede data kan ikke læses eller gendannes uden denne adgangskode**.

1. Hvis guiden User Initialization ikke er åben:

   Hvis du kører Windows XP Professional eller Home Edition, skal du klikke på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

   Hvis du kører Windows 2000, skal du klikke på **Start > Programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

2. Klik på **Next**.
3. Skriv og godkend en adgangskode til basisbrugeren, og klik derefter på **Next**.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

4. Klik på **Next** for at bekræfte indstillingerne.
5. Vælg de relevante sikkerhedsfunktioner, og klik på **Next**.
6. Klik på den relevante e-mail-klient for at markere den, og klik derefter på **Next**.
7. Klik på **Next** for at anvende krypteringscertifikatet.
8. Klik på **Next** for at bekræfte indstillingerne.
9. Klik på **Finish**.
10. Genstart computeren.

Gendannelse af krypterede data

Hvis du skal gendanne data efter udskiftning af ProtectTools-chippen, skal du have følgende:

- SPEmRecToken.xml – Emergency Recovery Token Key
- SPEmRecArchive.xml – skjult mappe, standardplacering: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools-adgangskoder
  - Opsætning
  - Take Ownership
  - Emergency Recovery Token
  - Basisbruger

1. Genstart computeren.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Skriv adgangskoden til opsætningen, og tryk derefter på **Enter**.
4. Tryk på en af piletasterne (Pil op eller Pil ned), og vælg et sprog. Tryk herefter på **Enter**.
5. Klik på den venstre eller højre piletast for at flytte til fanen **Security**, og benyt derefter Pil op eller Pil ned for at flytte til **Embedded Security Device**. Tryk på **Enter**.
6. Hvis kun én markering, **Embedded Security Device – Disable**, kan vælges:
   a. Tryk på venstre eller højre piletast for at flytte til **Embedded Security Device – Enable**. Tryk på **F10** for at godkende ændringen.
   b. Tryk på venstre eller højre piletast for at flytte til **File**. Tryk på Pil op eller Pil ned for at flytte til **Save Changes and Exit**. Tryk på **Enter**, og tryk derefter på **F10** for at godkende.
   c. Gå til trin 1.

   Hvis du har to valgmuligheder, skal du gå videre til trin 7.

7. Tryk på Pil op eller Pil ned for at flytte til **Reset to Factory Settings – Do Not Reset**. Tryk kun én gang på venstre eller højre piletast.

   Følgende meddelelse vises: Performing this action will reset the embedded security device to factory settings if settings are saved on exit. Press any key to continue.

   Tryk på **Enter**.

8. Du kan nu vælge **Reset to Factory Settings – Reset**. Tryk på **F10** for at godkende ændringen.
9. Tryk på venstre eller højre piletast for at flytte til **File**. Tryk på Pil op eller Pil ned for at flytte til **Save Changes and Exit**. Tryk på **Enter**, og tryk derefter på **F10** for at godkende.
10. Genstart computeren.
11. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

---

12. Skriv adgangskoden til opsætningen, og tryk derefter på **Enter**.
13. Tryk på en af piletasterne (Pil op eller Pil ned), og vælg et sprog. Tryk herefter på **Enter**.
14. Klik på den venstre eller højre piletast for at flytte til fanen **Security**, og benyt derefter Pil op eller Pil ned til at flytte til **Embedded Security Device**. Tryk på **Enter**.
15. Hvis markeringen i dialogboksen er **Embedded Security Device – Disable**, skal du bruge venstre eller højre piletast til at ændre den til **Embedded Security Device – Enable**. Tryk på **F10**.
16. Tryk på venstre eller højre piletast for at flytte til **File**. Tryk på Pil op eller Pil ned for at flytte til **Save Changes and Exit**. Tryk på **Enter**, og tryk derefter på **F10** for at godkende.

17. Når Windows kører:

    Hvis du kører Windows XP Professional eller Home Edition, skal du klikke på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

    Hvis du kører Windows 2000, skal du klikke på **Start > Programmer > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

18. Klik på **Next**.
19. Skriv en Take Ownership-adgangskode, og godkend den. Klik på **Next**.

Skriv omhyggeligt, da der af sikkerhedshensyn ikke vises tekst på skærmen, når du skriver.

20. Kontroller, at du har markeret Create a new recovery archive. Klik på **Browse** under **Recovery archive location**.
21. Godkend ikke standardfilnavnet. Skriv et nyt filnavn for at undgå at overskrive originalfilen.
22. Klik på **Save**, og klik derefter på **Next**.
23. Skriv og godkend en Emergency Recovery Token-adgangskode, og klik derefter på **Next**.
24. Sæt en diskette i, hvor du kan gemme Emergency Recovery Token Key. Klik på **Browse**, og vælg disketten.
25. Godkend ikke standardnøglenavnet. Skriv et nyt nøglenavn for at undgå at overskrive originalnøglen.
26. Klik på **Save**, og klik derefter på **Next**.
27. Klik på **Next** for at godkende indstillingerne, før sikkerhedsplatformen initialiseres.

En meddelelse om, at basisbrugerens nøgle ikke kan indlæses, vises muligvis. Klik ikke i meddelelsen. Den behandles senere i fremgangsmåden og lukker igen efter et par sekunder.

28. Klik på **Next** for at undgå konfiguration af lokale politikker.

29. Klik her for at fjerne markeringen i afkrydsningsfeltet **Start Embedded Security User Initialization Wizard**. Klik på **Finish**.
30. Højreklik på ikonet ProtectTools på værktøjslinjen, og klik på **Initialize Embedded Security restoration**.

    Nu startes guiden HP ProtectTools Embedded Security Initialization.
31. Klik på **Next**.
32. Sæt den diskette i, hvor du har gemt den originale Emergency Recovery Token Key. Klik på **Browse**, find Emergency Recovery Token, og dobbeltklik på den for at indtaste navnet i feltet. Standard er A:\SPEmRecToken.xml.
33. Skriv den originale Token-adgangskode, og klik på **Next**.
34. Klik på **Browse**, find det originale gendannelsesarkiv, og dobbeltklik på det for at indtaste navnet i feltet. Standard er C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Klik på **Next**.
36. Klik på den computer, der skal gendannes, og klik derefter på **Next**.
37. Klik på **Next** for at bekræfte indstillingerne.
38. Hvis guiden meddeler, at sikkerhedsplatformen er blevet gendannet, skal du gå videre til trin 39.

    Hvis guiden meddeler, at gendannelsen mislykkedes, skal du gå tilbage til trin 10. Kontroller adgangskoderne samt placering og navn på Emergency Recovery Token og placering og navn på arkivet omhyggeligt.
39. Klik på Finish.
40. Hvis du kører Windows XP Professional eller Home Edition, skal du klikke på **Start > Alle programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

    Hvis du kører Windows 2000, skal du klikke på **Start > Programmer > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
41. Klik på **Next**.
42. Klik på **Recover your basic user key**, og klik derefter på **Next**.

43. Marker en bruger, skriv den originale basisbruger-adgangskode til den pågældende bruger, og klik derefter på **Next**.
44. Klik på **Next** for at acceptere indstillingerne og godkende standardplaceringen for gendannede arkiver.

Trin 45 til 49 installerer basisbrugerens originale konfiguration igen.

45. Vælg de relevante sikkerhedsfunktioner, og klik på **Next**.
46. Klik på den relevante e-mail-klient for at markere den, og klik derefter på **Next**.
47. Klik på Encryption Certificate, og klik derefter på **Next** for at anvende det.
48. Klik på **Next** for at bekræfte indstillingerne.
49. Klik på **Finish**.
50. Genstart computeren.

FORSIGTIG: Sikkerhedskopiering af basisbrugerens adgangskode. **Krypterede data kan ikke læses eller gendannes uden denne adgangskode**.

DriveLock

DriveLock er en standardsikkerhedsfunktion, der forhindrer uautoriseret adgang til data på MultiBay-harddiske. DriveLock er implementeret som en udvidelse af Computer Setup. Det er kun tilgængeligt, når systemet finder DriveLock-kompatible harddiske.

DriveLock er beregnet til HP-kunder, for hvem datasikkerhed er af overordnet betydning. For disse kunder er prisen på harddisken og tabet af dataene, der er gemt på den, uden betydning sammenholdt med den skade, uautoriseret adgang til indholdet på disken kan forvolde. For at skabe balance mellem sikkerheden og det praktiske behov for at kunne oplyse en glemt adgangskode, følger HP's implementering af DriveLock en sikkerhedsstrategi med to adgangskoder. Den ene adgangskode skal angives og bruges af en systemadministrator, mens den anden adgangskode normalt vælges og anvendes af brugeren. Der findes ingen "bagdør", som kan bruges til at åbne drevet, hvis begge adgangskoder er gået tabt. Derfor er det sikrest at bruge DriveLock, når dataene på harddisken replikeres på virksomhedens informationssystem eller sikkerhedskopieres regelmæssigt.

Hvis begge DriveLock-adgangskoder går tabt, kan harddisken ikke bruges. For brugere, der ikke passer til den tidligere definerede kundeprofil, kan dette være en uacceptabel risiko. For brugere, der passer til kundeprofilen, er risikoen acceptabel af hensyn til de data, der gemmes på harddisken.

Brug af DriveLock

Indstillingen DriveLock vises i menuen Security i programmet Computer Setup. Brugeren får vist indstillinger til angivelse af hovedadgangskoden eller til at aktivere DriveLock. Der skal angives en brugeradgangskode for at aktivere DriveLock. Da den første konfiguration af DriveLock normalt udføres af systemets administrator, skal der først angives en hovedadgangskode. HP opfordrer systemadministratorer til at angive en hovedadgangskode, uanset om de har planer om at aktivere DriveLock eller bevare den deaktiveret. På den måde har administratoren mulighed for at ændre indstillinger for DriveLock, hvis drevet i fremtiden låses. Når hovedadgangskoden er angivet, kan systemadministratoren aktivere DriveLock eller vælge at bevare den deaktiveret.

POST kræver en adgangskode for at låse enheden op, hvis der findes en låst harddisk. POST beder ikke brugeren om at angive adgangskoden igen, hvis der er angivet en startadgangskode, og den svarer til enhedens brugeradgangskode. I modsat fald bliver brugeren bedt om at angive DriveLock-adgangskoden. Hoved- eller brugeradgangskoden kan anvendes. Brugerne har to forsøg til at angive en korrekt adgangskode. Hvis ingen af forsøgene lykkes, fortsætter POST, men der er ikke adgang til drevet.

Anvendelse af DriveLock

Den mest praktiske brug af DriveLock-sikkerhedsfunktionen er i et virksomhedsmiljø, hvor en systemadministrator udleverer MultiBay-harddiske til brug på nogle computere. Systemadministratoren er ansvarlig for at konfigurere MultiBay-harddisken, hvilket bl.a. medfører angivelse af DriveLock-hovedadgangskoden. Hvis brugeren glemmer sin brugeradgangskode, eller udstyret overdrages til en anden medarbejder, kan hovedadgangskoden altid bruges til at nulstille brugeradgangskoden og få adgang til harddisken igen.

HP anbefaler, at systemadministratorer i virksomheder, der vælger at aktivere DriveLock, også opretter virksomhedsregler for angivelse og vedligeholdelse af adgangskoder. Det skal gøres for at forhindre en situation, hvor en medarbejder tilsigtet eller utilsigtet angiver begge DriveLock-adgangskoder og forlader virksomheden. I det tilfælde vil harddisken ikke kunne bruges og skal udskiftes. På samme måde kan systemadministratorer, der ikke angiver en hovedadgangskode, være udelukket fra at få adgang til en harddisk ved rutinemæssig kontrol for uautoriseret software eller inventarkontrol og support.

Til brugere med mindre strenge sikkerhedskrav anbefaler HP ikke aktivering af DriveLock. Brugere i denne kategori omfatter hjemmebrugere, der normalt ikke opbevarer følsomme data på harddisken. Til disse brugere vil risikoen for at miste en harddisk, fordi begge adgangskoder glemmes, være større end værdien af de data, som DriveLock skal beskytte. Adgang til programmet Computer Setup og DriveLock kan begrænses med en adgangskode for opsætning. Ved at angive en adgangskode for opsætning, som slutbrugerne ikke får oplyst, kan systemadministratoren forhindre, at brugerne aktiverer DriveLock.

Smart Cover Sensor

Smart Cover Sensor, som findes på udvalgte modeller, er en kombination af hardware- og softwareteknologi, der kan advare om, at computerens dækplade eller sidepanel har været fjernet. Der er tre niveauer af beskyttelse, som beskrevet i tabellen herunder:

Beskyttelsesniveauer for Smart Cover Sensor

Niveau	Indstilling	Beskrivelse
Niveau 0	Disabled	Smart Cover Sensor er deaktiveret (standard).
Niveau 1	Notify User	Når computeren genstartes, vises en meddelelse på skærmen, der angiver, at dækpladen eller sidepanelet har været fjernet.
Niveau 2	Setup Password	Når computeren genstartes, vises en meddelelse på skærmen, der angiver, at dækpladen eller sidepanelet har været fjernet. Adgangskoden for opsætning skal angives, før du kan fortsætte.

✎ Disse indstillinger kan ændres med programmet Computer Setup. Se *Vejledning til Computer Setup (F10)* for at få flere oplysninger om computerens opsætning.

Indstilling af beskyttelsesniveauet for Smart Cover Sensor

Følg fremgangsmåden nedenfor for at indstille beskyttelsesniveauet for Smart Cover Sensor:

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security**, derefter **Smart Cover**, og følg derefter vejledningen på skærmen.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Smart Cover Lock

Smart Cover Lock er en funktion til fastlåsning af dækslet, der kontrolleres af softwareprogrammer og findes på visse HP-computere. Den skal forhindre uautoriseret adgang til computerens interne komponenter. Computere leveres med Smart Cover Lock i ulåst stilling.

FORSIGTIG: Låsen yder optimal sikkerhed, hvis du opretter en adgangskode for opsætning. Adgangskoden for opsætning forhindrer uautoriseret adgang til hjælpeprogrammet Computer Setup.

Smart Cover Lock er tilgængelig som ekstraudstyr på udvalgte systemer.

Låsning af Smart Cover Lock

Følg fremgangsmåden nedenfor for at aktivere og låse Smart Cover Lock:

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security**, og vælg derefter **Smart Cover** og indstillingen **Locked**.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Oplåsning af Smart Cover Lock

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security > Smart Cover > Unlocked**.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Brug af Smart Cover FailSafe-nøglen

Hvis Smart Cover Lock er aktiveret, og angivelsen af adgangskoden ikke deaktiverer låsen, skal du bruge en Smart Cover FailSafe-nøgle til at åbne computerens dæksel. Du skal bruge nøglen i følgende situationer:

- Strømafbrydelse
- Fejl ved opstart
- Pc-komponentfejl (f.eks. processor eller strømforsyning)
- Glemt adgangskode

FORSIGTIG: Smart Cover FailSafe-nøglen er et specialværktøj, som fås hos HP. Vær forberedt. Bestil denne nøgle, før du får brug for den, hos en autoriseret forhandler eller serviceudbyder.

Følg fremgangsmåden nedenfor for at få en FailSafe-nøgle:

- Kontakt en autoriseret HP-forhandler eller -serviceyder.
- Ring til det nummer, der er angivet i garantien.

Yderligere oplysninger om brug af Smart Cover FailSafe-nøglen finder du i *Hardwarevejledning*.

MBR-sikkerhed

MBR (Master Boot Record) indeholder oplysninger, der er nødvendige for at starte fra en disk og få adgang til de data, der er gemt på disken. Med MBR-sikkerhed forhindres utilsigtede eller skadelige ændringer af MBR, f.eks. pga. computervirus eller forkert brug af bestemte diskhjælpeprogrammer. Den giver dig desuden mulighed for at gendanne den sidste kendte fungerende MBR, hvis der konstateres ændringer af MBR, når systemet genstartes.

Følg fremgangsmåden nedenfor for at aktivere MBR-sikkerhed:

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren > Genstart computeren**, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security > Master Boot Record Security > Enabled**.
4. Vælg **Security > Save Master Boot Record**.
5. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Når MBR-sikkerhed er aktiveret, forhindrer BIOS enhver ændring i MBR på den disk, der aktuelt startes fra i fejlsikret tilstand i MS-DOS eller Windows.

De fleste operativsystemer kontrollerer adgangen til MBR på den aktuelle startdisk. BIOS kan ikke forhindre ændringer, der indtræffer, mens operativsystemet kører.

Hver gang computeren tændes eller genstartes, sammenligner BIOS MBR'en på den aktuelle startdisk med den MBR, der tidligere blev gemt. Hvis der konstateres ændringer, og hvis den aktuelle disk, der startes fra, er den samme som den, MBR'en tidligere blev gemt på, vises følgende meddelelse:

1999 – Master Boot Record has changed.

Tryk på en vilkårlig tast for at få adgang til opsætningsprogrammet og konfigurere MBR-sikkerhed.

Når du åbner programmet Computer Setup, skal du:

- Gemme MBR'en for den disk, der startes fra
- Gendanne den tidligere MBR, eller
- Deaktivere MBR-sikkerhedsfunktionen.

Du skal kende adgangskoden for opsætning, hvis den er defineret.

Hvis der konstateres ændringer, og hvis den aktuelle disk, der startes fra, **ikke** er den samme som den, MBR'en tidligere blev gemt på, vises følgende meddelelse:

2000 – Master Boot Record Hard Drive has changed.

Tryk på en vilkårlig tast for at få adgang til opsætningsprogrammet og konfigurere MBR-sikkerhed.

Når du åbner programmet Computer Setup, skal du:

- Gemme MBR'en for den disk, der startes fra, eller
- Deaktivere MBR-sikkerhedsfunktionen.

Du skal kende adgangskoden for opsætning, hvis den er defineret.

Skulle den MBR, du tidligere har gemt, været beskadiget, vises følgende meddelelse:

1998 – Master Boot Record has been lost.

Tryk på en vilkårlig tast for at få adgang til opsætningsprogrammet og konfigurere MBR-sikkerhed.

Når du åbner programmet Computer Setup, skal du:

- Gemme MBR'en for den disk, der startes fra, eller
- Deaktivere MBR-sikkerhedsfunktionen.

Du skal kende adgangskoden til opsætning, hvis den er defineret.

Inden partitionering eller formatering af den disk, der aktuelt startes fra

Kontroller, at MBR-sikkerhed er deaktiveret, før du foretager ændringer af formateringen eller partitioneringen af den aktuelle startdisk. Flere diskkommandoer, f.eks. FDISK og FORMAT, forsøger at opdatere MBR. Du modtager fejlmeddelelser fra diskhjælpeprogrammet eller en advarsel fra MBR-sikkerhed, næste gang computeren tændes eller genstartes, hvis MBR-sikkerhed er aktiveret, og du ændrer partitionering eller formatering af disken. Følg fremgangsmåden nedenfor for at deaktivere MBR-sikkerhed:

1. Tænd eller genstart computeren. Klik på **Start > Luk computeren >** Genstart computeren, hvis du kører Windows.
2. Tryk på tasten **F10**, så snart lampen på skærmen lyser grønt. Tryk eventuelt på **Enter** for at springe velkomstbilledet over.

Hvis du ikke trykker på tasten **F10** på det rigtige tidspunkt, skal du lukke computeren, tænde den og derefter trykke på tasten **F10** igen for at få adgang til hjælpeprogrammet.

3. Vælg **Security > Master Boot Record Security > Disabled**.
4. Klik på **File > Save Changes** og **Exit**, inden du afslutter.

Kabellås

Bagsiden af computeren er tilpasset en kabellås, så computeren fysisk kan fastgøres til et arbejdsområde.

Se *Hardwarevejledning*på cd'en *Documentation Library* for at se illustrerede instruktioner.

Fingeraftrykteknologi

HP's fingeraftrykteknologi har gjort adgangskoder overflødige og har samtidigt øget sikkerheden på netværk, gjort logonprocessen enklere og reduceret omkostningerne til vedligeholdelse. Den overkommelige pris betyder, at den ikke længere er forbeholdt avancerede organisationer med strenge sikkerhedskrav.

Understøttelsen af fingeraftrykteknologien varierer afhængigt af modellen.

Yderligere oplysninger finder du på http://h18000.www1.hp.com/solutions/security.

Fejlmeddelelse og gendannelse

Funktionerne til fejlmeddelelse and gendannelse kombinerer nyskabende hardware- og softwareteknologi, så tab af vigtige data forhindres, og eventuel nedetid formindskes.

Hvis der opstår en fejl, viser computeren lokale advarselsmeddelelser, der indeholder en beskrivelse af fejlen og eventuelle handlinger, som skal foretages. Derefter kan du få vist systemets status ved hjælp af HP Client Manager. Hvis computeren er tilsluttet et netværk, der styres af HP Insight Manager, HP Client Manager eller et andet systemadministrationsprogram, sender computeren også en fejlmeddelelse til netværksadministrationsprogrammet.

DPS (Drive Protection System)

DPS (Drive Protection System) er et diagnosticeringsværktøj, der er indbygget i de harddiske, som er installeret i visse HP-computere. DPS er designet til at afhjælpe de diagnosticeringsproblemer, der kan føre til uønsket udskiftning af harddiske.

Når HP-computere bliver bygget, testes hver harddisk ved hjælp af DPS, og en permanent fortegnelse over nøgleoplysningerne skrives på drevet. Hver gang DPS køres, skrives testresultaterne på harddisken. Serviceyderen bruger disse oplysninger til at afhjælpe de diagnosticeringsproblemer, der gjorde det nødvendigt at køre DPS-softwaren. Se under *Vejledning til fejlfinding* for at få vejledning i brug af DPS.

Strømstødstolerant strømforsyning

En integreret strømstødstolerant strømforsyning giver større pålidelighed, når computeren rammes af et uforudsigeligt strømstød. Denne strømforsyning er målt til at kunne modstå et strømstød på op til 2000 volt, uden at der opstår tab af systemtid og data.

Termisk sensor

Den termiske sensor er en hardware- og software-funktion, der sporer computerens interne temperatur. Funktionen viser en advarsel, hvis temperaturen overstiger den normale temperatur, hvilket giver dig tid til at gribe ind, før de interne komponenter beskadiges, eller data går tabt.

Indeks

T

U

W